Final Exam
CS 136
Spring, 2009

Answer all questions. There are 100 points total. Be sure to put your name on your test.

Multiple Choice questions. Each multiple choice question is worth 2 points. There is one best answer for each multiple choice question. Note that some of the questions are similar to questions on the midterm, but read them CAREFULLY, because none of them are exactly the same.

1. In symmetric cryptography, which of the following MUST be true:
    a. Encryption and decryption take the same amount of time
    b. Different algorithms are used for encryption and decryption
    c. Cryptographic operations are one-way, and not reversible
    d. The same key is used for encryption and decryption
2. If one uses electronic codebook (ECB) cryptographic mode to transmit a series of related blocks of data, which of the following is true?
    a. A single bit flip error in the first block will corrupt decryption of that block only
    b. A single bit flip error in the first block will corrupt decryption of the first and second block
    c. A single bit flip error in the first block will corrupt decryption of the first, second, and third blocks
    d. A single bit flip error in the first block will corrupt decryption of all blocks of the transmission
3. Which of the following statements is true about using asymmetric cryptography to provide authentication of the creator of a piece of information?
    a. It cannot be done
    b. It cannot be used for authentication of information stored for a long period of time
    c. Untrusted third parties can directly check the authentication
    d. It requires on-line use of a trusted third party

4. Alice and Bob share a symmetric cryptographic key that is known by nobody else, and both Alice and Bob know that. Alice encrypts a message to Bob with the shared key and transmits it to him. Which of the following does Bob NOT know, based on this cryptography, when he receives and decrypts this message, given that he knows someone other than himself created the message?
    a. The message could only have been created by Alice
    b. The encrypted message is unreadable by anyone except himself and Alice
    c. Both of the above
    d. None of the above
5. Personal Identification Numbers (PINs) are essentially passwords used as a second form of authentication for ATM cards and similar situations. A typical PIN is 4 characters long, and only uses the numerals from 0-9 in each position. But many of the keyboards used to enter PINs have two extra keys, often with a different symbol on each, such as a telephone pad's common inclusion of a * and # key. If PINs can also include either of these symbols, as well as the numerals, in each position, how many more PINs would be possible than with just the numerals?
    a. Around twice as many
    b. Around 20% more
    c. Around four times as many
    d. Around 16 times as many
6. A SYN flood exhausts what resource at its target?
    a. Ability of the machine's network card to handle incoming packets
    b. Entries in the process table
    c. Entries in the TCP connection table
    d. Processing power
7. Which of the following has NOT been a factor in making it hard to defend against distributed denial of service attacks?
    a. Ability of attackers to spoof their IP addresses
    b. Number of compromised machines available to perform attacks
    c. Ability of attackers to use arbitrary packets in the attack
    d. Inability of intrusion detection systems to detect such attacks
8. Which of the following is true of the use of link level encryption in a multihop network?
    a. It ensures that only the original sender and ultimate receiver can view the data in unencrypted form
    b. It requires fewer encryption and decryption operations than end-to-end encryption
    c. It can vary cryptographic algorithm strength to match individual components of the overall network path
    d. It is how a typical virtual private network (VPN) manages security across the Internet

9. Which of the following is NOT true of an IPSec Security Association (SA)?
    a. It describes a duplex connection
    b. It uses a particular set of cryptographic algorithms to protect the data it is related to
    c. It describes a connection between precisely two end points
    d. Its properties must be stored in databases at the parties making use of it
10. If you were implementing Tor-style onion routing using IPSec to provide all necessary cryptographic services, which of the following statements would be true?
    a. You would only need to use IPSec's authentication features
    b. ESP in transport mode would be a good match for your needs
    c. ESP in tunnel mode would be a good match for your needs
    d. You would want to avoid using IPSec Security Parameter Indices (SPIs) to prevent tracing of the packets
11. Source address filtering can be used either on packets coming into or going out of an edge network. Which of the following is true for a typical edge network?
    a. The same set of packets can be properly filtered in either direction
    b. More different source addresses can be filtered on packets leaving the edge network and going into the Internet than packets coming from the Internet going into the edge network
    c. More different source addresses can be filtered on packets coming from the Internet going into the edge network than packets leaving the edge network and going into the Internet
    d. If you perform filtering in one of the two directions, you must not perform it in the other or you will interrupt proper flow of packets
12. Which of the following is true of firewalls?
    a. An application gateway firewall will probably need more processing power than a filtering gateway firewall
    b. If you use an application gateway firewall, you will not need to update it regularly
    c. If you install a reverse firewall, you will have no need for a filtering firewall
    d. Transparency is an undesirable property for a firewall
13. In a normal multi-firewall configuration, which of the following is true of the DMZ?
    a. It contains any machines you keep outside your outermost firewall
    b. It is the area inside your innermost firewall
    c. It is between your outermost firewall and innermost firewall
    d. It contains portable machines that have not yet been validated to allow them any network access

14. Which of the following is true of virtual private networks?
    a. They use cryptography to provide a similar security effect as a direct protected network link
    b. Their main purpose is to guarantee quality of service in the face of denial of service attacks
    c. They are primarily used to allow secure communications within a honeypot that is emulating multiple machines on one real machine
    d. They require use of TPM technology at all endpoint machines to achieve their goals
15. In the context of network security, what is backscatter?
    a. Damage done to legitimate traffic when a denial of service defense drops traffic coming from some source
    b. Evidence of IP spoofing obtained by watching traffic arriving at unallocated IP addresses
    c. A method of obtaining entropy to create cryptographic keys to be used by IPSec
    d. A method botnet controllers use to communicate within the botnet
16. Which of the following is not an important failure mode for an intrusion detection system?
    a. False positives
    b. Subversion errors
    c. False negatives
    d. Synchronization errors
17. Which of the following is true of anomaly detection based intrusion detection systems?
    a. They can only detect problems they are already aware of
    b. They may be susceptible to training attacks
    c. They are the basis of most commercial intrusion detection systems available today
    d. They are only usable for network-based intrusion detection, not host-based intrusion detection
18. One dimension along which computer viruses are classified is what kind of computer resource they infect. Which of the following is not a virus classification of this kind?
    a. Polymorphic viruses
    b. TSR viruses
    c. Multipartite viruses
    d. Macro viruses
19. Which of the following is NOT a reason why it is hard for defenders to deal with botnets?
    a. Legal issues
    b. Difficulty of finding and analyzing copies of the botnet code
    c. Scale
    d. Difficulty in tracing the controlling user of the botnet

20. What is the main purpose of a rootkit?
    a. To obtain and maintain complete control of a compromised computer
    b. To spread to other machines
    c. To steal private information
    d. To fool users into running malicious executables on their machines
21. The term TOCTOU is relevant to which kind of program security flaw?
    a. Buffer overflows
    b. Misplaced trust
    c. Race conditions
    d. Variable initialization
22. Experts in secure C/C++ programming recommend that you do not use the `scanf()` function. Why?
    a. It fails to ensure that its cryptographic key is chosen properly
    b. It is often susceptible to buffer overflows
    c. It is likely to cause improper synchronization between its first and second parameters
    d. It tends to cause race conditions
23. Which of the following is most likely to cause a security problem in the use of a random number generator?
    a. Use of a pseudorandom number generator
    b. Generating a random number based on variations in hardware performance
    c. Using a cryptographic hash to generate a random number
    d. Generating a random number based on user input
24. Which of the following was NOT a reason for the ultimate failure of the Orange Book approach to security ratings?
    a. Slow time to market of rated products
    b. Lack of confidence that the ratings actually meant systems were suitably secure
    c. Lack of universal trust in the parties performing the security evaluations
    d. Too much generality in the security models it covered
25. What is the primary purpose of an attack tree?
    a. Tracing spoofed packets through the Internet
    b. Ensuring proper input validation
    c. Describing improper behavior for misuse detection methods of intrusion detection systems
    d. Threat modeling

26. Which of the following is the fundamental result of Cohen's theoretical analysis of virus detection?
    a. Detecting an arbitrary virus in an arbitrary program is undecidable
    b. The number of tests one must perform to detect a set of virus signatures in an arbitrary program is NP-complete
    c. The rate of infection of a computer virus in a particular environment is a logarithmically increasing function
    d. The path of a virus' infection through a set of programs is Hamiltonian
27. What is a trusted computing base (TCB)?
    a. A Common Criteria term describing the system being evaluated
    b. Special hardware that can provide remote attestations about the software running on a machine
    c. The set of protection mechanisms within a computing system that are responsible for enforcing a security policy
    d. A formally verified operating system kernel that ensures access controls are properly handled
28. In a typical case of cross-site scripting, which party is attacking which party?
    a. A client is attacking a server
    b. A client is attacking another client
    c. A server is attacking a client
    d. A server is attacking another server
29. What of the following is NOT true of Tor-style onion routing?
    a. Data is encrypted multiple times
    b. The packet takes the most direct path from the source to the destination
    c. Each intermediate router does not know if the next hop is the final destination
    d. Proper key management is critical to the goals of the system
30. Which of the following is NOT an important issue for using capabilities for access control?
    a. Preventing improper copying of capabilities
    b. Handling revocation
    c. Figuring out a given subject's security domain
    d. Identifying all subjects that can access a resource

Short Answer questions. Answer each of these in 2-3 sentences. Each question is worth 8 points.

1. Is an intrusion prevention system more like a honeypot or a firewall? Why?

2. What does the quality of its random number generator have to do with the ability of a worm to spread quickly?

3. Cryptography can be used for many things. For example, it could be used to encrypt data to be archived on a tape for many years, or it could be used to protect a critical message being sent across the Internet. Are the issues of key selection the same or different for these two cases?

4. Recent proof-of-concept experiments have shown that malware can potentially infect firmware in peripheral devices. What changes will this observation require in procedures for cleaning up infected machines?

5. Why is error handling an important issue for writing secure code?